UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/625,548	07/25/2000	Laurence Hamid	12-50US	7154

7590 07/01/2004

Gordon Freedman
Freedman & Associates
117 Centrepointe Drive
Suite 350
Nopean, ON K2G 5X3
CANADA

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	3

DATE MAILED: 07/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/625,548	Applicant(s) HAMID ET AL.	
	Examiner Justin T. Darrow	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-21 and 27-29 is/are rejected.

7)☒ Claim(s) 22-26 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 25 July 2000 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 have been examined.

Drawings

2. This application lacks formal drawings. The informal drawings filed in this application are acceptable for examination purposes. Formal drawings must be made in reply to this Office action. See 37 CFR 1.85(a).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 11 recites the limitation "the secured data" twice in page 19, line 2. There is insufficient antecedent basis for this limitation in the claim.

5. Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 15 recites the limitation "the secured data" twice in page 20, line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 1-10, 12-14, 16-21, and 27-29 are rejected under 35 U.S.C. 102(a) as being anticipated by Global Transaction Company (Renner), International Application Publication No. WO 01/82190 A1.

As per claim 1, Renner discloses a method authorizing a user in communication with a workstation (see page 6, lines 8-21; figure 3, items 5, 6, 20, and 101; a user in communication a personal computer (PC) and with a Web server) comprising:

automatically determining at least an available user information entry device in communication with the workstation (see page 3, lines 4-8; a password log-in, a smart card, smart card reader, and biometric reader operable to identify user through installation software);

determining user authorization methods each requiring data only from available user information entry devices from a plurality of user authorization methods (see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader if those options are being used);

providing user authorization information in accordance with one of the determined user authorization methods (see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader if those options are being used); and

registering the user authorization information provided against stored data to perform at least one of identifying and authorization the user (see page 7, lines 23-25; page 8, lines 1-4; retrieve evidence to support claimed identity and provides this and the claimed identity to the identity authority; page 8, lines 5-9; identity authority examines the evidence and generates a response upon a comparison; page 8, lines 8-14; where a successful comparison results in an identity notification and authorization to access resources such as a requested Web page).

As per claim 2, Renner further depicts:

a plurality of available user information entry devices (see page 3, lines 4-8; a password log-in, a smart card, smart card reader, and biometric reader operable to identify user).

As per claim 3, Renner then describes:

selecting from the determined user authorization methods the one method wherein the provided user authorization information is provided in accordance with the selected one method (see page 4, lines 5-7; a Federal government Web site requiring biometric verification; see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader).

As per claim 4, Renner also points out:

providing to the user a list of the determined user authorization methods in which the user selects from the provided list, a single user authorization method (see page 6, lines 9-13; access is predominantly controlled in accordance with specific rules and criteria related to individual users and transactions; page 9, lines 17-25; where a Web side provides scripts to use the identity verification service on the user's PC such that user chooses a script method for identification).

As per claim 5, Renner additionally elaborates:

determining security information associated with the user and with the selected user authorization method, the security information different for different user authorization methods (see page 15, lines 1-5; in the order of relative importance and security needed for the transaction used, the tiered verification functions of identification, verified identification, and verified transaction signature may correspond to password log-in, smart card verification and biometric (e.g. fingerprint) identification demands).

As per claim 6, Renner then describes:

that each user authorization method is associated with a security level and in which at least one of identifying and authorizing the user with the associated security level (see page 4, lines 3-12; the Federal government requiring biometric verification for an applicant of benefits and an online drug retailer requiring certification for a prescribing doctor's identity and authorization; see page 15, lines 1-5; in the order of relative importance and security needed for the transaction used, the tiered verification functions of identification, verified identification, and verified transaction signature may correspond to password log-in, smart card verification and biometric (e.g. fingerprint) identification demands).

As per claim 7, Renner alternatively discusses:

each determined method is supported absent further installation of software components (see page 3, lines 8-11; software may be stand alone for exclusive use with the system).

As per claim 8, Renner moreover suggests:

retrieving a security key from a key storage location in dependence on upon the registration (see page 13, lines 6-9; figure 3, items 11, 12, and 104; the user enrolling in a verification system by providing a user name and password to be filed in an authority's database; see page 15, lines 11-13; upon the user's providing the user name and password, the authority retrieves the user identity profile data containing the user name and password).

As per claim 9, Renner further elaborates:

that the security key is an encryption key (see page 14, lines 3-5; that the security key retrieved for authorization is in the form of an encryption key used to encrypt authorization data exchanged between the user's PC and the ID authority).

As per claim 10, Renner additionally specifies:

that the security key is a password (see page 13, lines 6-9; figure 3, items 11, 12, and 104; the user enrolling in a verification system by providing a user name and password to be filed in an authority's database; see page 15, lines 11-13; upon the user's providing the user name and password, the authority retrieves the user identity profile data containing the user name and password).

As per claim 12, Renner also mentions:

upon access to secured data prompting an individual using the workstation to provide user authorization information (see page 13, lines 18-22; prompting the user to comply with an identity demand; and

registering the user authorization information provided against stored data in accordance with a user authorization method to perform one of providing access to the secured data and denying access to the secured data in dependence upon the registration results (see page 15, lines 18-25; the ID Authority either approves or disapproves the user identity resulting in authority to conduct secure communications exchanging secure data.

As per claim 13, Renner illustrates a method of authorizing a user in communication with a workstation (see page 6, lines 8-21; figure 3, items 5, 6, 20, and 101; a user in communication a personal computer (PC) and with a Web server) comprising:

providing a plurality of supported user authorization methods and associated security levels for each user authorization method (see page 15, lines 1-5; in the order of relative importance and security needed for the transaction used, the tiered verification functions of identification, verified identification, and verified transaction signature may correspond to password log-in, smart card verification and biometric (e.g. fingerprint) identification demands);

providing user authorization information to the workstation (see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader if those options are being used);

determining from the plurality of supported user authorization methods an authorization method requiring data only from the provided user authorization information (see page 7, lines 23-25; page 8, lines 1-6; from the claimed identity data collected from any or the smart card and biometric reader, the identity authority examines the evidence provided in the packet the user's PC sends in accordance with the method for the data); and

registering the user authorization information provided against stored data to perform at least one of identifying and authorizing the user with the associated level of security (see page 8, lines 5-9; if the method succeeds, the user is registered and provided a unique verification code).

As per claim 14, Renner further points out:

selecting from the determined user authorization methods the one method wherein the provided user authorization information is provided in accordance with the selected one method (see page 4, lines 5-7; a Federal government Web site requiring biometric verification; see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader).

As per claim 16, Renner elaborates:

determining security information associated with the user and the security level, where the security information is different for different user authorization methods (see page 4, lines 3-12; the Federal government requiring biometric verification for an applicant of benefits and an online drug retailer requiring certification for a prescribing doctor's identity and authorization; see page 15, lines 1-5; in the order of relative importance and security needed for the transaction used, the tiered verification functions of identification, verified identification, and verified transaction signature may correspond to password log-in, smart card verification and biometric (e.g. fingerprint) identification demands).

As per claim 17, Renner moreover suggests:

retrieving a security key from a key storage location in dependence on upon the registration (see page 13, lines 6-9; figure 3, items 11, 12, and 104; the user enrolling in a verification system by providing a user name and password to be filed in an authority's database; see page 15, lines 11-13; upon the user's providing the user name and password, the authority retrieves the user identity profile data containing the user name and password).

As per claim 18, Renner further elaborates:

that the security key is an encryption key (see page 14, lines 3-5; that the security key retrieved for authorization is in the form of an encryption key used to encrypt authorization data exchanged between the user's PC and the ID authority).

As per claim 19, Renner additionally specifies:

that the security key is a password (see page 13, lines 6-9; figure 3, items 11, 12, and 104; the user enrolling in a verification system by providing a user name and password to be filed in an authority's database; see page 15, lines 11-13; upon the user's providing the user name and password, the authority retrieves the user identity profile data containing the user name and password).

As per claim 20, Renner also mentions:

upon initiating access to secured data prompting an individual using the workstation to provide user authorization information (see page 13, lines 18-22; prompting the user to comply with an identity demand; and

registering the user authorization information provided against stored data in accordance with a user authorization method to perform one of providing access to the secured data and denying access to the secured data in dependence upon the registration results (see page 15, lines 18-25; the ID Authority either approves or disapproves the user identity resulting in authority to conduct secure communications exchanging secure data.

As per claim 21, Renner depicts a method of authorizing a user in communication with a workstation (see column 1, lines 41-50; an authorized user interacting with a computer) comprising:

providing a plurality of user authorization methods, some requiring user authorization information from more than one data input device (see Abstract; figure 3, items 1, 2, and 3; any single or combination of password log-in, smart card, or biometric routines may be required for authorization);

providing user authorization information (see page 7, lines 23-25; collecting claimed identity data);

registering the provided user authorization information against data stored in a database of user authorization data (page 15, lines 11-15; figure 3, items 12 and 104; comparing the user entered authorization information with data from the user identity profile in the ID authority's database);

when the data matches the stored data within predetermined limits, determining a security level for the individual in dependence upon the provided user authorization information and the plurality of user authorization methods (see page 15, lines 19-22; with an approved secure identity, communications proceed with level of identification of 1c, 2c, or 3c); and

authorizing the user access within limits based upon determined security level (see page 15, lines 23-25; limiting access to a user with a sufficiently verified identity from making purchases in excess of a given value because they do not have such authority to do so).

As per claim 27, Renner then describes:

selecting a user authorization method from the plurality of user authorization methods during execution (see page 4, lines 5-7; a Federal government Web site requiring biometric verification); and

providing user authorization information in accordance with the selected user authorization method (see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader).

As per claim 28, Renner also discloses:

automatically determining the presence or absence of user information entry devices in communication with the workstation (see page 3, lines 4-8; a password log-in, a smart card, smart card reader, and biometric reader operable to identify user through installation software); and

determining user authorization methods from the plurality of user authorization methods that require data only from user information entry devices which are present (see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader if those options are being used).

As per claim 29, Renner then describes:

selecting a user authorization method from the plurality of determined authorization methods (see page 4, lines 5-7; a Federal government Web site requiring biometric verification); and

providing user authorization information in accordance with the selected user authorization method (see page 7, lines 23-25; page 8, lines 1-4; software components on the PC collect claimed identity data manipulating the smart card and biometric reader).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 11 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Global Transaction Company (Renner), International Application Publication No. WO 01/82190 A1 as applied to claims 1 and 13, respectively, above, and further in view of Lamber, U.S. Patent No. 6,193,153 B1.

Renner discloses the methods of claim 1 and 13. He describes:

the Web server periodically checking the identification verification performed by the identity authority (see page 10, lines 15-22); and

registering the verification performed against stored verification stored to provide access or deny access to secured data (see page 10, lines 15-22)

However, he does not explicitly teach, at intervals, prompting an individual to provide authorization information.

Lamber illustrates:

at intervals prompting an individual using the workstation to provide user authorization information (see column 9, lines 31-39; figure 4, items 500 and 560; at random and/or predetermined intervals, prompting the user to physically interact with the event converter by pushing buttons, touching a key pad, facing a camera, or speaking; see column 9, lines 18-21; resulting in the non-intrusive identification of the user); and

registering the user authorization information provided against stored data to perform one of providing access to secured data and denying access to secured data in dependence upon registration results (see column 2, lines 32-35; to grant or deny an identified user access to directories or e-mail access).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Renner with the prompting at intervals to provide user authorization information for continuous monitoring of biometric data of users of restricted or secure areas for verification purposes (see column 2, lines 16-18).

Allowable Subject Matter

10. Claims 22-26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Flyntz, U.S. Patent No. 6,389,542 B1, discloses a multilevel computer security system including multiple security subsystems
- Atl et al., U.S. Patent No. 6,389,542 B1 describes a method for identifying a person for secured transactions with wearable security devices

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the

application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

June 27, 2004

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100